

WHAT IS CLAIMED IS:

Sub
a1

1 1. A network multiplexing and tunneling system, comprising at least two
2 devices connected across a network by a secure connection created at a user-level,
3 wherein the secure connection is a single encrypted Secure Sockets Layer (SSL)
4 Transmission Control Protocol (TCP) connection, each of the devices authenticates
5 the other device after the secure connection is opened, and at least one of the devices
6 multiplexes other connections through the secure connection after both the devices
7 have been authenticated.

1 2. The system of claim 1, wherein the other connections are selected from
2 a group comprising Transmission Control Protocol (TCP) and UDP (User Datagram
3 Protocol) connections.

1 3. The system of claim 1, wherein the secure connection is symmetric.

1 4. The system of claim 1, wherein either endpoint of the secure
2 connection can receive connection requests.

1 5. The system of claim 1, wherein either endpoint of the secure
2 connection can receive data.

1 6. The system of claim 1, further comprising means for maintaining send
2 buffers on each endpoint.

1 7. The system of claim 1, further comprising means for forwarding data
2 through the secure connection when there are sufficient send buffers for receiving the
3 forwarded data on the other endpoint.

1 8. The system of claim 1, further comprising means for queuing data
2 received at each endpoint.

1 9. The system of claim 8, further comprising means for dispatching the
2 queued data at each endpoint to its final destination.

1 10. The system of claim 9, further comprising means for acknowledging
2 receipt of the data after the queued data is dispatched to its final destination, thereby
3 tracking usage of buffers at the endpoint.

1 11. The system of claim 1, further comprising means for buffering data
2 transmitted through the multiplexed other connections for flow control through the
3 secure connection.

1 12. The system of claim 1, further comprising means for resolving domain
2 names through the secure connection.

1 13. The system of claim 1, further comprising means for operating the
2 secure connection according to a mode selected from a group comprising a standalone
3 proxy mode, a packet filter mode, and a SOCKetS server (SOCKS) mode.

1 14. The system of claim 1, wherein the endpoints comprise a Portal and a
2 Gate.

1 15. The system of claim 14, wherein the Gate comprises a server executed
2 by a firewall bastion host computer.

1 16. The system of claim 14, wherein the Portal comprises a client executed
2 by a user's computer.

1 17. The system of claim 1, further comprising means for accessing an
2 Intranet from the Internet using the secure connection.

1 18. The system of claim 17, further comprising means for creating a
2 connection from a Portal on a client computer on the Internet to a Gate on a firewall
3 bastion host computer on the Intranet through the secure connection.

1 19. The system of claim 17, further comprising means for creating a
2 connection from a Portal on a client computer on the Internet to a proxy on a
3 firewall bastion host computer on the Intranet through the secure connection and
4 from the proxy to a Gate on a host computer on the Intranet through the secure
5 connection.

1 20. The system of claim 17, further comprising means for creating a
2 connection from a Portal on a client computer on the Internet to a packet filter on a
3 firewall bastion host computer on the Intranet through the secure connection and
4 from the packet filter to a Gate on a host computer on the Intranet through the secure
5 connection.

1 21. The system of claim 1, further comprising means for accessing the
2 Internet from an Intranet using the secure connection.

1 22. The system of claim 21, further comprising means for creating a
2 connection from a Portal on a client computer on the Intranet to a Gate on a host
3 computer on the Internet through the secure connection.

1 23. The system of claim 21, further comprising means for creating a
2 connection from a Portal on a firewall bastion host computer on the Intranet to a
3 host computer on the Internet through the secure connection.

1 24. The system of claim 21, further comprising means for creating a
2 connection from a Portal on a client computer on the Intranet to a proxy on a
3 firewall bastion host computer on the Intranet through the secure connection and
4 from the proxy to a Gate on a host computer on the Internet through the secure
5 connection.

1 25. The system of claim 21, further comprising means for creating a
2 connection from a Portal on a client computer on the Intranet to a packet filter on a
3 firewall bastion host computer on the Intranet through the secure connection and
4 from the packet filter to a Gate on a host computer on the Internet through the secure
5 connection.

1 26. The system of claim 1, further comprising means for accessing a first
2 Intranet from a second Intranet across the Internet using the secure connection.

1 27. The system of claim 26, further comprising means for creating a
2 connection from a Portal on a client computer on the first Intranet to a Gate on a
3 firewall bastion host computer on the first Intranet through the secure connection,
4 and from the Gate on the firewall bastion host computer on the first Intranet through
5 the Internet to a Gate on a firewall bastion host computer on the second Intranet
6 through the secure connection, and from the Gate on the firewall bastion host
7 computer on the second Intranet to a host computer on the second Intranet through
8 the secure connection.

1 28. The system of claim 1, wherein records are exchanged between the
2 endpoints of the secure connection.

1 29. The system of claim 28, wherein the records are selected from a group
2 comprising: UsherOpen, UsherOpenReply, UsherSend, UsherClose, UsherSendUdp,
3 UsherAck, UsherEnd, and UsherRST records.

1 30. The system of claim 29, wherein the UsherOpen records are sent by a
2 Portal to a Gate to open a Transmission Control Protocol (TCP) connection.

1 31. The system of claim 29, wherein the UsherOpenReply records are sent
2 by a Gate to a Portal to respond to an UsherOpen record.

1 32. The system of claim 29, wherein the UsherSend records are sent by
2 either a Gate or a Portal to transmit data therebetween.

1 33. The system of claim 29, wherein the UsherAck records are sent by
2 either a Gate or a Portal to acknowledge a receipt of data therebetween.

1 34. The system of claim 29, wherein the UsherAck records are not send
2 when data received by either a Gate or a Portal is queued prior to being forwarded to
3 its destination.

1 35. The system of claim 29, wherein the UsherAck records are sent only
2 when data received by either a Gate or a Portal has been forwarded to its destination.

1 36. The system of claim 29, wherein the UsherClose records are sent by
2 either a Gate or a Portal to terminate a session.

1 37. The system of claim 29, wherein the UsherSendUdp records are sent
2 by either a Gate or a Portal to transmit UDP (User Datagram Protocol) packets
3 therebetween.

1 38. The system of claim 29, wherein the UsherEnd records are sent by
2 either a Gate or a Portal to terminate a multiplexed other connection.

1 39. The system of claim 29, wherein the UsherRST records are sent by
2 either a Gate or a Portal to reset a multiplexed other connection.

1 40. A transmission media communicating data via a secure connection
2 created at a user-level between two endpoints in a network, wherein the secure
3 connection is a single encrypted Secure Sockets Layer (SSL) Transmission Control
4 Protocol (TCP) connection, each of the endpoints authenticates the other device after
5 the secure connection is opened, and at least one of the endpoints multiplexes other
6 connections through the secure connection after both the endpoints have been
7 authenticated.

1 41. The transmission media of claim 40, wherein the other connections are
2 selected from a group comprising Transmission Control Protocol (TCP) and UDP
3 (User Datagram Protocol) connections.

1 42. The transmission media of claim 40, wherein the secure connection is
2 symmetric.

1 43. The transmission media of claim 40, wherein either endpoint of the
2 secure connection can receive connection requests.

1 44. The transmission media of claim 40, wherein either endpoint of the
2 secure connection can receive data.

1 45. The transmission media of claim 40, further comprising maintaining
2 send buffers on each endpoint.

1 46. The transmission media of claim 40, further comprising forwarding
2 data through the secure connection when there are sufficient send buffers for
3 receiving the forwarded data on the other endpoint.

1 47. The transmission media of claim 40, further comprising queuing data
2 received at each endpoint.

1 48. The transmission media of claim 47, further comprising dispatching
2 the queued data at each endpoint to its final destination.

1 49. The transmission media of claim 48, further comprising
2 acknowledging receipt of the data after the queued data is dispatched to its final
3 destination, thereby tracking usage of buffers at the endpoint.

1 50. The transmission media of claim 40, further comprising buffering data
2 transmitted through the multiplexed other connections for flow control through the
3 secure connection.

1 51. The transmission media of claim 40, further comprising resolving
2 domain names through the secure connection.

1 52. The transmission media of claim 40, further comprising operating the
2 secure connection according to a mode selected from a group comprising a standalone
3 proxy mode, a packet filter mode, and a SOCKetS server (SOCKS) mode.

1 53. The transmission media of claim 40, wherein the endpoints comprise a
2 Portal and a Gate.

1 54. The transmission media of claim 53, wherein the Gate comprises a
2 server executed by a firewall bastion host computer.

1 55. The transmission media of claim 53, wherein the Portal comprises a
2 client executed by a user's computer.

1 56. The transmission media of claim 40, further comprising accessing an
2 Intranet from the Internet using the secure connection.

1 57. The transmission media of claim 56, further comprising creating a
2 connection from a Portal on a client computer on the Internet to a Gate on a firewall
3 bastion host computer on the Intranet through the secure connection.

1 58. The transmission media of claim 56, further comprising creating a
2 connection from a Portal on a client computer on the Internet to a proxy on a
3 firewall bastion host computer on the Intranet through the secure connection and
4 from the proxy to a Gate on a host computer on the Intranet through the secure
5 connection.

1 59. The transmission media of claim 56, further comprising creating a
2 connection from a Portal on a client computer on the Internet to a packet filter on a
3 firewall bastion host computer on the Intranet through the secure connection and
4 from the packet filter to a Gate on a host computer on the Intranet through the secure
5 connection.

1 60. The transmission media of claim 40, further comprising accessing the
2 Internet from an Intranet using the secure connection.

1 61. The transmission media of claim 60, further comprising creating a
2 connection from a Portal on a client computer on the Intranet to a Gate on a host
3 computer on the Internet through the secure connection.

1 62. The transmission media of claim 60, further comprising creating a
2 connection from a Portal on a firewall bastion host computer on the Intranet to a
3 host computer on the Internet through the secure connection.

1 63. The transmission media of claim 60, further comprising creating a
2 connection from a Portal on a client computer on the Intranet to a proxy on a
3 firewall bastion host computer on the Intranet through the secure connection and
4 from the proxy to a Gate on a host computer on the Internet through the secure
5 connection.

1 64. The transmission media of claim 60, further comprising creating a
2 connection from a Portal on a client computer on the Intranet to a packet filter on a
3 firewall bastion host computer on the Intranet through the secure connection and
4 from the packet filter to a Gate on a host computer on the Internet through the secure
5 connection.

1 65. The transmission media of claim 40, further comprising accessing a
2 first Intranet from a second Intranet across the Internet using the secure connection.

1 66. The transmission media of claim 65, further comprising creating a
2 connection from a Portal on a client computer on the first Intranet to a Gate on a
3 firewall bastion host computer on the first Intranet through the secure connection,
4 and from the Gate on the firewall bastion host computer on the first Intranet through
5 the Internet to a Gate on a firewall bastion host computer on the second Intranet

6 through the secure connection, and from the Gate on the firewall bastion host
7 computer on the second Intranet to a host computer on the second Intranet through
8 the secure connection.

1 67. The transmission media of claim 40, wherein records are exchanged
2 between the endpoints of the secure connection.

1 68. The transmission media of claim 67, wherein the records are selected
2 from a group comprising: UsherOpen, UsherOpenReply, UsherSend, UsherClose,
3 UsherSendUdp, UsherAck, UsherEnd, and UsherRST records.

1 69. The transmission media of claim 68, wherein the UsherOpen records
2 are sent by a Portal to a Gate to open a Transmission Control Protocol (TCP)
3 connection.

1 70. The transmission media of claim 68, wherein the UsherOpenReply
2 records are sent by a Gate to a Portal to respond to an UsherOpen record.

1 71. The transmission media of claim 68, wherein the UsherSend records
2 are sent by either a Gate or a Portal to transmit data therebetween.

1 72. The transmission media of claim 68, wherein the UsherAck records are
2 sent by either a Gate or a Portal to acknowledge a receipt of data therebetween.

1 73. The transmission media of claim 68, wherein the UsherAck records are
2 not send when data received by either a Gate or a Portal is queued prior to being
3 forwarded to its destination.

1 74. The transmission media of claim 68, wherein the UsherAck records are
2 sent only when data received by either a Gate or a Portal has been forwarded to its
3 destination.

1 75. The transmission media of claim 68, wherein the UsherClose records
2 are sent by either a Gate or a Portal to terminate a session.

1 76. The transmission media of claim 68, wherein the UsherSendUdp
2 records are sent by either a Gate or a Portal to transmit UDP (User Datagram
3 Protocol) packets therebetween.

1 77. The transmission media of claim 68, wherein the UsherEnd records are
2 sent by either a Gate or a Portal to terminate a multiplexed other connection.

1 78. The transmission media of claim 68, wherein the UsherRST records
2 are sent by either a Gate or a Portal to reset a multiplexed other connection.

1 79. A method for network multiplexing and tunneling, comprising:
2 (a) opening a single Transmission Control Protocol (TCP) connection at a
3 user-level between at least two endpoints in the network;
4 (b) establishing a Secure Sockets Layer (SSL) over the opened Transmission
5 Control Protocol (TCP) connection;
6 (c) mutually authenticating each of the endpoints of the SSL TCP connection;
7 and
8 (d) multiplexing other connections through the secure connection once both
9 of the endpoints have been authenticated.

1 80. The method of claim 79, wherein the other connections are selected
2 from a group comprising Transmission Control Protocol (TCP) and UDP (User
3 Datagram Protocol) connections.

1 81. The method of claim 79, wherein the secure connection is symmetric.

1 82. The method of claim 79, wherein either endpoint of the secure
2 connection can receive connection requests.

1 83. The method of claim 79, wherein either endpoint of the secure
2 connection can receive data.

1 84. The method of claim 79, further comprising maintaining send buffers
2 on each endpoint.

1 85. The method of claim 79, further comprising forwarding data through
2 the secure connection when there are sufficient send buffers for receiving the
3 forwarded data on the other endpoint.

1 86. The method of claim 79, further comprising queuing data received at
2 each endpoint.

1 87. The method of claim 86, further comprising dispatching the queued
2 data at each endpoint to its final destination.

1 88. The method of claim 87, further comprising acknowledging receipt of
2 the data after the queued data is dispatched to its final destination, thereby tracking
3 usage of buffers at the endpoint.

1 89. The method of claim 79, further comprising buffering data transmitted
2 through the multiplexed other connections for flow control through the secure
3 connection.

1 90. The method of claim 79, further comprising resolving domain names
2 through the secure connection.

1 91. The method of claim 79, further comprising operating the secure
2 connection according to a mode selected from a group comprising a standalone proxy
3 mode, a packet filter mode, and a SOCKetS server (SOCKS) mode.

1 92. The method of claim 79, wherein the endpoints comprise a Portal and
2 a Gate.

1 93. The method of claim 92, wherein the Gate comprises a server executed
2 by a firewall bastion host computer.

1 94. The method of claim 92, wherein the Portal comprises a client
2 executed by a user's computer.

1 95. The method of claim 79, further comprising accessing an Intranet from
2 the Internet using the secure connection.

1 96. The method of claim 95, further comprising creating a connection
2 from a Portal on a client computer on the Internet to a Gate on a firewall bastion
3 host computer on the Intranet through the secure connection.

1 97. The method of claim 95, further comprising creating a connection
2 from a Portal on a client computer on the Internet to a proxy on a firewall bastion
3 host computer on the Intranet through the secure connection and from the proxy to
4 a Gate on a host computer on the Intranet through the secure connection.

1 98. The method of claim 95, further comprising creating a connection
2 from a Portal on a client computer on the Internet to a packet filter on a firewall
3 bastion host computer on the Intranet through the secure connection and from the
4 packet filter to a Gate on a host computer on the Intranet through the secure
5 connection.

1 99. The method of claim 79, further comprising accessing the Internet
2 from an Intranet using the secure connection.

1 100. The method of claim 99, further comprising creating a connection
2 from a Portal on a client computer on the Intranet to a Gate on a host computer on
3 the Internet through the secure connection.

1 101. The method of claim 99, further comprising creating a connection
2 from a Portal on a firewall bastion host computer on the Intranet to a host computer
3 on the Internet through the secure connection.

1 102. The method of claim 99, further comprising creating a connection
2 from a Portal on a client computer on the Intranet to a proxy on a firewall bastion
3 host computer on the Intranet through the secure connection and from the proxy to
4 a Gate on a host computer on the Internet through the secure connection.

1 103. The method of claim 99, further comprising creating a connection
2 from a Portal on a client computer on the Intranet to a packet filter on a firewall
3 bastion host computer on the Intranet through the secure connection and from the
4 packet filter to a Gate on a host computer on the Internet through the secure
5 connection.

1 104. The method of claim 79, further comprising accessing a first Intranet
2 from a second Intranet across the Internet using the secure connection.

1 105. The method of claim 104, further comprising creating a connection
2 from a Portal on a client computer on the first Intranet to a Gate on a firewall
3 bastion host computer on the first Intranet through the secure connection, and from
4 the Gate on the firewall bastion host computer on the first Intranet through the
5 Internet to a Gate on a firewall bastion host computer on the second Intranet through
6 the secure connection, and from the Gate on the firewall bastion host computer on
7 the second Intranet to a host computer on the second Intranet through the secure
8 connection.

1 106. The method of claim 79, wherein records are exchanged between the
2 endpoints of the secure connection.

1 107. The method of claim 106, wherein the records are selected from a
2 group comprising: UsherOpen, UsherOpenReply, UsherSend, UsherClose,
3 UsherSendUdp, UsherAck, UsherEnd, and UsherRST records.

1 108. The method of claim 107, wherein the UsherOpen records are sent by
2 a Portal to a Gate to open a Transmission Control Protocol (TCP) connection.

1 109. The method of claim 107, wherein the UsherOpenReply records are
2 sent by a Gate to a Portal to respond to an UsherOpen record.

1 110. The method of claim 107, wherein the UsherSend records are sent by
2 either a Gate or a Portal to transmit data therebetween.

1 111. The method of claim 107, wherein the UsherAck records are sent by
2 either a Gate or a Portal to acknowledge a receipt of data therebetween.

1 112. The method of claim 107, wherein the UsherAck records are not send
2 when data received by either a Gate or a Portal is queued prior to being forwarded to
3 its destination.

1 113. The method of claim 107, wherein the UsherAck records are sent only
2 when data received by either a Gate or a Portal has been forwarded to its destination.

1 114. The method of claim 107, wherein the UsherClose records are sent by
2 either a Gate or a Portal to terminate a session.

1 115. The method of claim 107, wherein the UsherSendUdp records are sent
2 by either a Gate or a Portal to transmit UDP (User Datagram Protocol) packets
3 therebetween.

1 116. The method of claim 107, wherein the UsherEnd records are sent by
2 either a Gate or a Portal to terminate a multiplexed other connection.

1 117. The method of claim 107, wherein the UsherRST records are sent by
2 either a Gate or a Portal to reset a multiplexed other connection.